(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: 0 267 647 A2

(12) EUROPEAN PATENT APPLICATION

(21) Application number: 87202133.2

(51) Int. Cl.4: H04L 9/00

(22) Date of filing: 05.11.87

(30) Priority: 11.11.86 NL 8602847

(43) Date of publication of application: 18.05.88 Bulletin 88/20

(84) Designated Contracting States: AT BE CH DE FR GB IT LI SE

(71) Applicant: N.V. Philips' Gloeilampenfabrieken
Groenewoudseweg 1
NL-5621 BA Eindhoven(NL)

(72) Inventor: Jansen, Cornelis Johannes Adrianus
c/o INT. OCTROOIBUREAU B.V. Prof. Holstlaan 6
NL-5656 AA Eindhoven(NL)

(74) Representative: De Jongh, Cornelis Dominicus et al
INTERNATIONAAL OCTROOIBUREAU B.V.
Prof. Holstlaan 6
NL-5656 AA Eindhoven(NL)

(54) Enciphering/deciphering method and arrangement for performing the method.

(57) The invention relates to a method of enciphering information-containing digital data signals with the aid of enciphering keys and of deciphering a message thus enciphered, utilizing the same key. For usages in which high demands are made on the quality of enciphering the conventional method - the EX-OR adding together of clear text and key text on a bit basis - has shortcomings. The invention has for its object to provide a very reliable method with which furthermore the propagation of errors caused by any transmission errors is prevented. This is accomplished in that the (clear) text characters to be enciphered are processed using an enciphering key which is derived from a key text and that the nature of the processing operation performed on the clear text characters is determined by an instruction command which is also derived from the key text.

EP 0 267 647 A2

"Enciphering/deciphering method and arrangement for performing the method"

The invention relates to a method of enciphering information-containing digital data signals with the aid of enciphering keys and of deciphering a message thus enciphered, utilizing the same key.

Such a method is disclosed in, for example, European Patent Application 0011615. The key usually consists of a long sequence of binary numbers (ones and zeroes). Cryptographic text is obtained by adding the key (mostly exclusive-OR per bit) to the clear text to be enciphered. This cryptographic text is transferred or transmitted to a receiver where the original, clear text is obtained by subtracting the same key as utilized in the transmitter from the received cryptographic text. For uses where very high demands are imposed on the quality of the enciphering this method has many shortcomings.

It is an object of the invention to provide a method by means of which clear text can be enciphered very reliably and error propagation due to any type of transmission errors is prevented. According to the invention, the enciphering method of the type defined in the opening paragraph is characterized in that the data signals to be enciphered are processed with the aid of an enciphering key which is derived from a key text and in that the nature of the processing operation performed on the data signals to be enciphered is determined by an instruction command which is also derived from the key text.

This method has the advantage that the number of processing operations which can be performed on the clear text/key combination is (very) large. In contradistinction thereto, only two processing operations are possible in the conventional system, namely adding (modulo-2) and adding followed by inverting. A further advantage of the method according to the invention is that no error propagation occurs: one incorrectly received cryptographic text character does not produce more than one faulty character in the clear text.

The invention is based on the recognition that a "spoofer" must know the processing function used to be successful in "spoofing". As a - in the statistical sense - unique function is selected for each character to be enciphered, the changes the "spoofer" is successful is inversely proportional to the number of possible functions to the power of the number of characters to be spoofed and consequently can be reduced to any arbitrary small extent.

It is advantageous for the processing operations performed to include the cyclic changes from 0 to (n-1) bits of the bits of the character to be enciphered the character to be enciphered comprising n bits.

It is advantageous for the processing operations performed to include the modulo-2^m addition of the key character or groups of bits thereof to the character to be enciphered or groups of bits thereof, it being possible for m to assume any value between 1 and n.

The invention further relates to an arrangement for performing the method. According to the invention, this arrangement is characterized in that it includes a control arrangement, an input of which is connected to the key text generator and a first output of which is connected to the enciphering unit for providing a key character and a second output of which is also connected to the enciphering unit for providing the instruction command and that the enciphering arrangement includes means for enciphering a character of the digital data signals under the control of the instruction command and the key character.

Further particulars and advantages will become apparent from the description of an embodiment given with reference to the accompanying Figure. Therein:

Figure 1: is a circuit diagram of an enciphering arrangement according to the invention; and

Figure 2: shows an example of the bit patterns such as they occur in the enciphering arrangement of Figure 1.

Figure 1 shows an arrangement for character-based enciphering utilizing the what is commonly referred to as the "steamcipher" principle. Characters are sets of bits comprising a plurality of bits, these characters together constituting an alphabet such as, for example, the ASCII or the BAUDOT alphabet. The clear text to be enciphered is applied to an enciphering unit 11 via a bus 10 having, for example, the same number of signal wires as there are bits in a character. By processing the clear text, the crypto text appears at the output 12 of enciphering unit 11. The output 12 is, for example, also constituted by a bus having the same number of signal wires as there are bits in a crypto character. Processing the clear text is effected by a control arrangement 13 connected to the enciphering unit 11. The control arrangement has a first output 14 via which a what is commonly referred to as a key K is applied to the enciphering unit 11. The key K has a sequency of binary numbers ("ones" and "zeroes") in a pseudo-random sequence which is generated in a manner still further to be described. The key does not contain a stationary pattern of binary numbers but always utilizes a variable pattern.

In addition, the control arrangement 13 has a

second output 15 via which an instruction command can be transferred to the enciphering arrangement. The instruction command specifies the nature of the processing function to be performed by the enciphering arrangement 11 on the clear text and on the key. Let the clear text be P ("plain text") and the key be K ("key") and the enciphered text be C ("crypto text") then the instruction command specifies the function F by means of which the crypto text C is obtained by subjecting the clear text P to the processing operation F utilizing key K. Expressed in a formula:

$C = F_k(p)$ (1)

The inverse operation is effected in the receiver and the received crypto-text is deciphered in accordance with:

$P = F_k^{-1}$ (C) (2)

From this it appears that the operating function F should preferably be of a type which is "easily" invertable when K is known.

The key and the instruction command are derived from a pseudo-random key text generator 17. This generator includes a data-standard-enciphering unit 19 (DES) in the OFB-mode (Output feedback mode) which, as is shown in the Figures, is a self-contained streamcipher. DES data-standard-enciphering units are known per se. See, for example, the article by W. Diffie and M.E. Hellman, entitled "Privacy and authentication: and introduction to cryptography", published in Proc. IEEE Vol. 67, No. 3, March 1979, pages 397-427, more specifically Figure 13 and the associated text.

A key K is applied to a first input 20 of the data-standard-enciphering unit 19. On the basis thereof the data-standard-enciphering unit 19 generates a pseudo-random key text of, for example, 64 bits at an output 18. This text is applied to both the control arrangement 13 and - via bus 22 - to an input of register 21. When a subsequent pseudo-random key text is generated, this is based on (a portion of) the previous text and the key K. For that purpose an output of the register 21 is connected to a second input 23 of the data-standard-enciphering unit 19.

Although for the pseudo-random key text generator 17 shown in Figure 1 use is made of a DES OFB streamcipher such an embodiment is absolutely not essential to the invention: any other embodiment of the key text generator 17 is equally suitable provided a signal of the desired type is available at output 18.

The enciphering arrangement 13 operates as follows: A key character is derived from the key text applied via bus 18. If the clear text to be enciphered consists of eight-bit words, a key character of likewise 8 bits is, for example, selected. These bits may, for example, be the first eight (or the last or the centre etc.) bits of the key text applied via bus 18. An instruction command is also derived from the applied text. The instruction command is merely a number (for example a 7-bit binary number) which can assume arbitrary values in a predetermined, accurately defined field. It is, for example, possible for the number to assume all the integral values between 0 and 127. The value of the number determines, as is described in the foregoing, the nature of the processing operation the enciphering unit 11 will perform.

A plurality of functions may serve as the operating function F_k. One possibility might be the cyclic interchange of the bits of a character of the clear text through n positions, n being determined by a number of bits of the instruction command (so a maximum of 7 positions if the character consists of eight bits). The characters 11011001 "rotated" through 4 positions then becomes 10011101. A second possibility might be the modulo-2^m addition of a clear text character and a key text character depending on the value of a number of bits of the instruction command. Thus, the eight bits of the character of the clear text might be added modulo-4 in four groups of 2 bits to the likewise four groups of 2 bits each of the key text character. Continuing along this line, the following eight possibilities would consist for eight-bit characters, namely:

a) 8 bits modulo-2

b) 4 times 2 bits modulo-4

c) 2 times 3 bits modulo-8 and 1 time 2 bits modulo-4

d) 2 times 4 bits modulo-16

e) 1 time 5 bits modulo-32 and 1 time 3 bits modulo-8

f) 1 time 6 bits modulo-64 and 1 time 2 bits modulo-4

g) 1 time 7 bits modulo-128 and 1 time 1 bit modulo-2

h) 1 time 8 bits modulo-256 Together with further combinations a total of more than 100 variations are possible for a 8-bit character. The number of possibilities increases exponentially with the length of the character.

Classes of processing functions other than the functions described here are alternatively possible. The processing functions may alternatively be combined, as will be demonstrated on the basis of the following example (Figure 2). The character P (8 bits) to be enciphered is 01101011. This character is first subjected to a cyclic interchange through 2 bits procedure. This results in the character r(P), namely 10101101. This rotation can be indicated by three bits (3 bits are required to indicate a rotation through 0-7 bits) of the instruction command.

The clear text character thus rotated is there-

after processed as follows. The clear text character r(P) is divided into three groups, namely two groups of three bits each and one 2-bit group. The key text character k (11010011) is divided in a similar manner into three groups. Thereafter the corresponding groups are added together modulo-8 or modulo-4, as the case may be, (in conformity with the above-indicated possibility (c)). Also this adding operation can be defined by three bits of the instruction command (c is one of the above-mentioned 8 possibilities a to h, inclusive). The resulting crypto text character C then is 01111100. This character is transmitted to a receiver and deciphered there.

This manner of enciphering has the advantage that an error caused, for example, by an interference in the receiver, cannot result in more than one faulty clear text character being received. So no error propagation occurs as does occur in many other enciphering methods.

The enciphering unit 11 and the control arrangement 13 can be realised in the form of what are commonly referred to as wired logic modules. A more attractive possibility is, however the realisation of the enciphering unit by means of the arithmetical and logic unit (ALU) of a micro-processor and to implement the control arrangement as a program for that micro-processor.

Claims

1. A method of enciphering information-containing digital data signals with the aid of enciphering keys and of deciphering a message thus enciphered, utilizing the same key, characterized in that the data signals to be enciphered are processed with the aid of an enciphering key derived from a key text and in that the nature of the processing operation performed on the data signals to be enciphered is determined by an instruction command which is also derived from the key text.

2. An enciphering/deciphering method as claimed in Claim 1, characterized in that the processing operations performed include the cyclic interchange from 0 to (n-1) bits of the bits of the characters to be enciphered, the character to be enciphered comprising n bits.

3. An enciphering/deciphering method as claimed in Claim 1, characterized in that the processing operations performed include the modulo-2^m addition of the key character or groups of bits thereof to the characters to be enciphered or to groups of bits thereof, wherein $1 \leq m \leq n$.

4. An arrangement for performing the method as claimed in any one of the preceding Claims, the arrangement including an enciphering unit (11) and a key text generator coupled thereto, the enciphering unit (11) having an input (10) for receiving clear digital data signals, characterized in that the arrangement includes a control arrangement (13) an input of which is connected to the key text generator (17) and a first output of which is connected to the enciphering unit (11) for providing (14) a key character and a second output of which is also connected to the enciphering unit (11) for providing (15) the instruction command and that the enciphering arrangement includes means for enciphering a character of the digital data signals under the control of the instruction command and the key character.

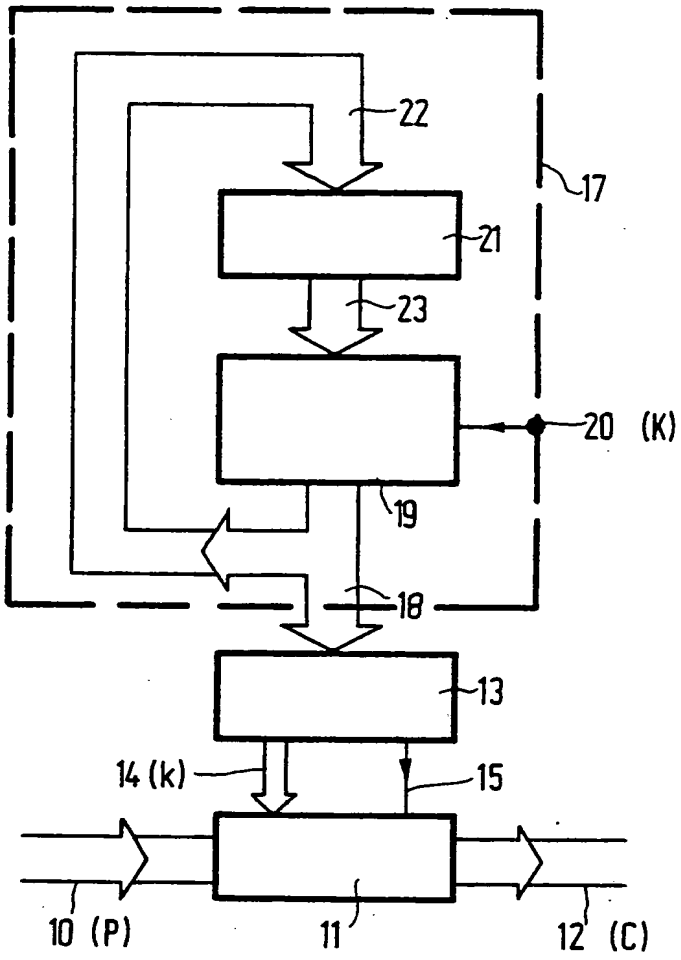
22
17
21
23
20 (K)
19
18
13
14 (k)
15
10 (P)
11
12 (C)

FIG.1

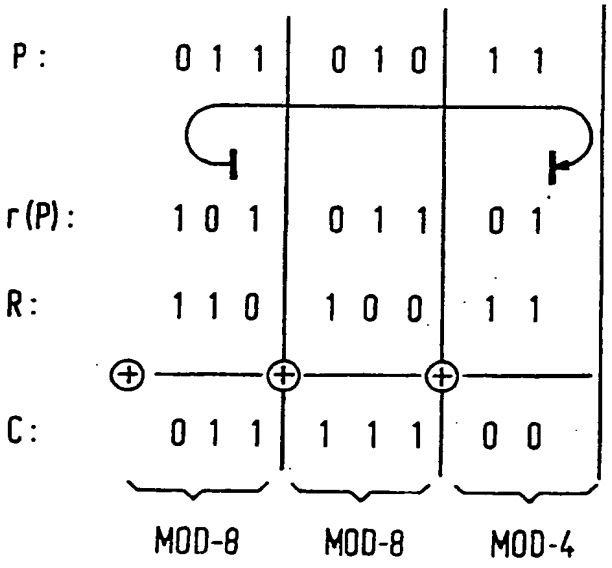
P :
0 1 1
0 1 0
1 1
r(P) :
1 0 1
0 1 1
0 1
R :
1 1 0
1 0 0
1 1
C :
0 1 1
1 1 1
0 0
MOD-8
MOD-8
MOD-4

FIG.2

European Patent Office

EUROPEAN SEARCH REPORT

Application Number

EP 87 20 2133

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int. Cl.4)
Y	US-A-4 157 454 (BECKER) * Abstract; column 3, line 63 - column 4, line 4; tables I,II; figure 1 *	1-4	H 04 L 9/00
Y	US-A-3 796 830 (SMITH) * Column 3, lines 17-37; claims 1,3,4 *	1-4	
Y	EP-A-0 105 553 (STAAT DER NEDERLANDEN) * Page 4, lines 21-29; claim 1; figures 4,5 *	3	

TECHNICAL FIELDS SEARCHED (Int. Cl.4)

H 04 L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	22-08-1989	SNELL T.

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P0401)

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 267 647**
A3

(12) EUROPEAN PATENT APPLICATION

(21) Application number: **87202133.2**

(51) Int. Cl.⁴: **H04L 9/00**

(22) Date of filing: **05.11.87**

(30) Priority: **11.11.86 NL 8602847**

(43) Date of publication of application:
18.05.88 Bulletin 88/20

(84) Designated Contracting States:
AT BE CH DE FR GB IT LI SE

(88) Date of deferred publication of the search report:
08.11.89 Bulletin 89/45

(71) Applicant: **N.V. Philips' Gloeilampenfabrieken**
Groenewoudseweg 1
NL-5621 BA Eindhoven(NL)

(72) Inventor: **Jansen, Cornelis Johannes Adrianus**
c/o INT. OCTROOIBUREAU B.V. Prof. Holstlaan 6
NL-5656 AA Eindhoven(NL)

(74) Representative: **De Jongh, Cornelis Dominicus et al**
INTERNATIONAAL OCTROOIBUREAU B.V.
Prof. Holstlaan 6
NL-5656 AA Eindhoven(NL)

(54) Enciphering/deciphering method and arrangement for performing the method.

(57) The invention relates to a method of enciphering information-containing digital data signals with the aid of enciphering keys and of deciphering a message thus enciphered, utilizing the same key. For usages in which high demands are made on the quality of enciphering the conventional method - the EX-OR adding together of clear text and key text on a bit basis - has shortcomings. The invention has for its object to provide a very reliable method with which furthermore the propagation of errors caused by any transmission errors is prevented. This is accomplished in that the (clear) text characters to be enciphered are processed using an enciphering key which is derived from a key text and that the nature of the processing operation performed on the clear text characters is determined by an instruction command which is also derived from the key text.

EP 0 267 647 A3